CyAN

Cybersecurity
Advisors
Network

Cyber (In)Securities

Issue #129

NEWS:

1. Latin American Orgs Face 40% More Attacks Than Global Average

Original Source: Dark Reading by Nate Nelson

Organizations in Latin America are experiencing a surge in cyberattacks, facing 40% more incidents than the global average.

This alarming trend underscores the unique cybersecurity challenges in the region, exacerbated by rapid digital transformation and targeted attacks by sophisticated cybercriminals.

Latin American businesses are urged to significantly enhance their cyber defenses and implement comprehensive security strategies.

Emphasising the need for advanced threat detection systems and robust cybersecurity training, these measures are crucial to mitigate escalating threats and protect vital infrastructures.

CyberSecurity Advisors Network

NEWS:

2. Nearly 12,000 API keys and passwords found in AI training dataset

Original Source: BleepingComputer by Ionut Ilascu

A concerning discovery in an AI training dataset has surfaced nearly 12,000 API keys and passwords, highlighting significant security vulnerabilities.

This incident demonstrates the risks associated with using real-world data in machine learning projects without stringent verification and cleansing processes. The inadvertent exposure of sensitive credentials could lead to substantial security breaches, emphasising the urgent need for robust data sanitisation protocols and enhanced privacy protection measures in AI development.

Organisations must prioritise tightening their data handling practices to prevent similar vulnerabilities and protect sensitive information from potential cyber threats.

CyberSecurity Advisors Network

NEWS:

3. DHS says CISA won’t stop looking at Russian cyber threats

Original Source: Cyberscoop by Tim Starks

The Department of Homeland Security (DHS) has reaffirmed its commitment to monitoring Russian cyber threats, as stated by the Cybersecurity and Infrastructure Security Agency (CISA).

This comes amid escalating global tensions and increasing cyber activities from state-sponsored groups. CISA emphasises the continuous need for vigilance and proactive measures to counter these threats effectively.

The agency's ongoing focus on Russian cyber operations underscores the critical importance of national cyber defence strategies in protecting U.S. infrastructures and maintaining cybersecurity resilience.

CyberSecurity Advisors Network

NEWS:

4. Hackers Exploit AWS Misconfigurations to Launch Phishing Attacks via SES and WorkMail

Original Source: The Hacker News by Ravie Lakshmanan

Hackers are exploiting misconfigurations in Amazon Web Services (AWS), specifically targeting SES and WorkMail, to launch sophisticated phishing attacks.

This tactic allows cybercriminals to send seemingly legitimate emails from trusted domains, significantly increasing the likelihood of successful scams.

The incidents highlight the critical vulnerabilities associated with cloud services and the necessity for stringent security practices.

Organisations using AWS are urged to conduct regular security audits and tighten configurations to thwart these phishing schemes and protect sensitive data from being compromised.

CyberSecurity Advisors Network

NEWS:

5. EU's New Product Liability Directive & Its Cybersecurity Impact

Original Source: Dark Reading by Jatin Mannepalli

The EU's New Product Liability Directive introduces significant changes with profound implications for cybersecurity across member states.

This legislation extends liability to include digital products, compelling manufacturers to ensure higher security standards to avoid legal repercussions. It's designed to protect consumers from potential harms caused by digital products and services, including those related to cybersecurity breaches.

The directive not only aims to enhance consumer protection but also pushes companies to adopt more rigorous cybersecurity measures, thereby elevating the overall security posture within the digital marketplace.

CyberSecurity Advisors Network

NEWS:

6. Microsoft unveils finalized EU Data Boundary as European doubt over US grows

Original Source: The Register by Richard Speed

Microsoft has officially finalized the EU Data Boundary, responding to increasing European concerns about data privacy and the handling of information by U.S. entities.

This strategic move ensures that all personal data from European customers will be stored and processed within EU borders, aligning with stringent EU data protection regulations.

The implementation of this boundary aims to mitigate legal risks, enhance data sovereignty, and strengthen trust among European users. It reflects Microsoft's commitment to addressing privacy concerns and adapting to global demands for more localised and secure data management practices.

CyberSecurity Advisors Network

NEWS:

7. UK watchdog to investigate TikTok and Reddit over use of children’s data

Original Source: The Guardian By Robyn Vinter

The UK watchdog is set to investigate TikTok and Reddit for their handling of children's data, raising significant concerns about privacy and protection online.

This inquiry highlights potential violations of data protection laws intended to safeguard minors from misuse of their personal information on these platforms. The investigation aims to ensure that both social media giants adhere strictly to legal standards, emphasising the importance of robust age verification processes and transparent data usage policies.

This action underscores the growing urgency to protect young users in the digital landscape, where personal data is often vulnerable to exploitation.

CyberSecurity Advisors Network

NEWS:

8. C++ creator calls for help to defend programming language from 'serious attacks'

Original Source: The Register by Thomas Claburn

Bjarne Stroustrup, the esteemed creator of C++, has urgently called for support to defend the programming language from what he terms as 'serious attacks'.

These attacks compromise the integrity and efficiency of C++, potentially undermining its reliability and performance for developers globally.

Stroustrup emphasises the critical importance of rallying the programming community to protect C++ and maintain its foundational role in software development, impacting a vast array of applications across various industries. He stresses the potential long-term implications for technological innovation and software integrity if these challenges are not addressed effectively.

CyberSecurity Advisors Network

NEWS:

9. LinkedIn scam emails warning

Original Source: ITWire by Gordon Peters

Amid rising cybersecurity concerns, LinkedIn users are increasingly targeted by sophisticated scam emails that mimic official communications.

These phishing attempts are designed to steal personal data by convincing users to click on malicious links that appear to be legitimate LinkedIn updates.

Security experts are sounding the alarm, highlighting the growing prevalence and sophistication of these scams. They strongly urge users to be vigilant, to verify the authenticity of messages, and to understand the risks to their personal information online amid these evolving cyber threats, emphasising the need for enhanced digital literacy.

CyberSecurity Advisors Network

NEWS:

10. Extreme online violence may be linked to rise of ‘0 to 100’ killers, experts say

Original Source: The Guardian by Rachel Hall

Experts are increasingly concerned about the link between extreme online violence and the emergence of '0 to 100' killers, individuals who rapidly escalate from no criminal background to committing severe acts of violence.

This phenomenon is being studied as part of broader efforts to understand how digital environments influence offline behaviour.

Researchers are examining patterns in online activity that may predict these sudden violent outbursts, suggesting that early intervention could prevent potential tragedies.

The focus is on creating tools and strategies to identify and mitigate these risks before they manifest in real-world violence.

CyberSecurity Advisors Network

March 6th webinar This Week!

Breaking the Cycle: Combating Online IBSA for a Safer Digital Experience

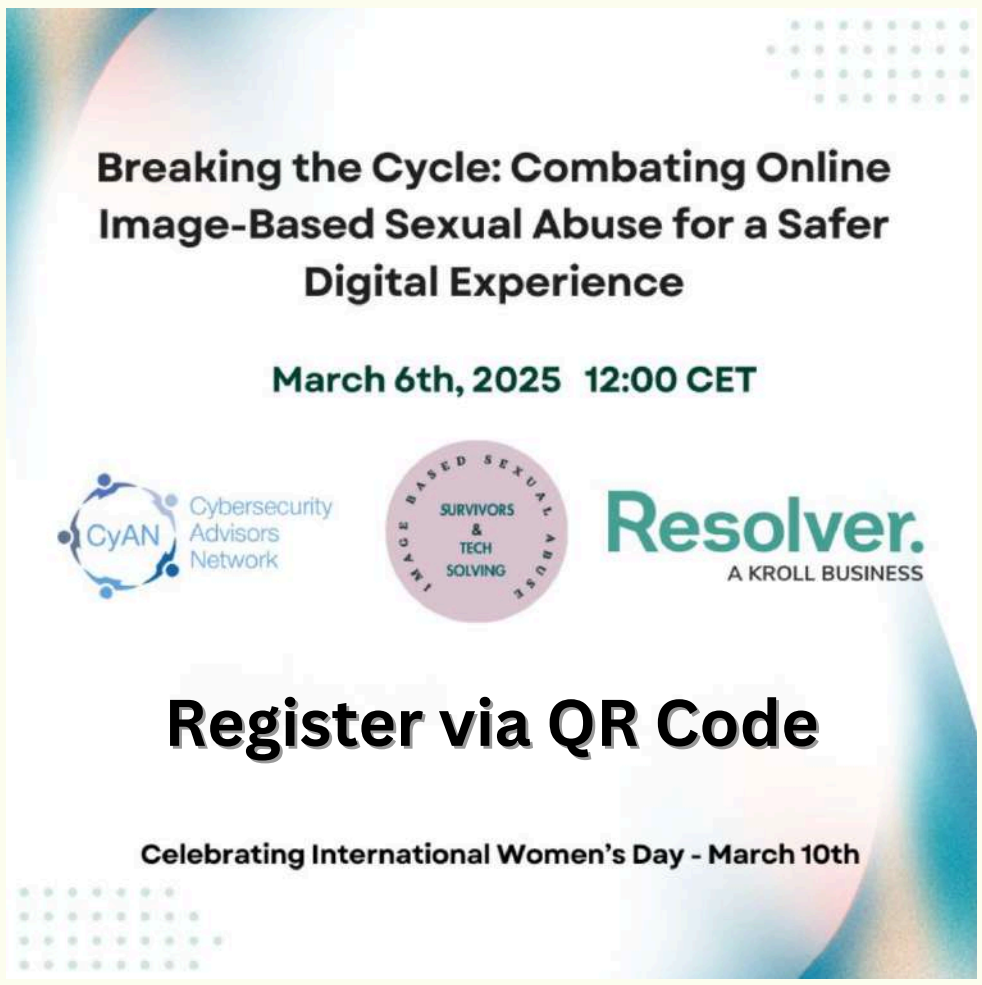


Image-Based Sexual Abuse (IBSA) is a growing threat—one that deeply impacts individuals, communities, and the very fabric of online trust. It's time to take action.

Join Cybersecurity Advisors Network (CyAN), Resolver Trust & Safety, and STISA (Survivors & Tech Solving Image-based Sexual Abuse) for a powerful webinar that brings together leading experts and changemakers to tackle this urgent issue head-on.

This webinar will feature speakers:
Caroline Humer, Henry 'H' Adams, Robbert Hoving, Dr Silvia Semenzin and CyAN's Kim Chandler McDonald

Cybersecurity Advisors Network

NEWS:

11. Ransomware gangs exploit Paragon Partition Manager bug in BYOVD attacks

Original Source: BleepingComputer by Bill Toulas

Ransomware gangs are exploiting a vulnerability in Paragon Partition Manager to conduct BYOVD (Bring Your Own Vulnerable Driver) attacks.

This technique allows attackers to bypass security measures by using legitimate but flawed drivers. Security researchers warn that this vulnerability is particularly dangerous because it enables ransomware to gain deep system access without immediate detection.

The exploit has been used in several high-profile ransomware campaigns, highlighting the critical need for updates and patches to protect against such sophisticated cyber threats.

Efforts are underway to mitigate the risk by providing timely security updates and educating users on the importance of maintaining software integrity.

CyberSecurity Advisors Network

NEWS:

12. Trump administration retreats in fight against Russian cyber threats

Original Source: The Guardian by Stephanie Kirchgaessner

The Trump administration has reportedly pulled back from aggressive cyber operations against Russian cyber threats, sparking concerns among cybersecurity experts.

This decision reflects a shift in strategy that may leave critical US infrastructure more vulnerable to attacks.

Experts argue that reducing proactive cyber defense measures could embolden adversaries and lead to increased cyber espionage and disruptive attacks targeting vital sectors.

The move has drawn criticism for potentially weakening the US's stance on cyber defense at a time when robust measures are needed most to counter growing global cyber threats.

CyberSecurity Advisors Network

NEWS:

13. Tarlogic Discovers Security Flaw Allowing Eavesdropping on Private Conversations Via Bluetooth Headset Microphone

Original Source: IT Security Guru by Daniel Tannenbaum

Tarlogic Security has uncovered a significant flaw in Bluetooth technology that allows eavesdropping on private conversations via Bluetooth headset microphones.

This vulnerability can be exploited without alerting the device owner, making it a serious privacy concern.

Researchers at Tarlogic warn that this flaw not only breaches individual privacy but also poses a risk to corporate security if sensitive business discussions are intercepted.

The discovery has prompted calls for immediate updates to Bluetooth security protocols to prevent such vulnerabilities and protect users from potential espionage.

CyberSecurity Advisors Network

NEWS:

14. SolarWinds CISO says security execs are ‘nervous’ about individual liability for data breaches

Original Source: Cyberscoop by Derek B. Johnson

Tim Brown, the CISO of SolarWinds has voiced concerns that security executives are becoming increasingly nervous about being held personally liable for data breaches.

This anxiety is driven by the rising frequency and severity of cyber attacks, which are putting immense pressure on security frameworks.

Brown emphasises the need for robust security measures and proactive risk management strategies to protect against potential breaches.

Additionally, there is a call for clearer regulations and support systems to help security professionals manage these challenges without the fear of personal repercussions.

CyberSecurity Advisors Network

NEWS:

15. Attackers Could Hack Smart Solar Systems and Cause Serious Damages

Original Source: Security Affairs by Pierluigi Paganini

Security researchers have raised alarms over vulnerabilities in smart solar systems that could be exploited by hackers to cause serious damage.

These systems, integral to renewable energy grids, can be remotely accessed if not properly secured, allowing attackers to manipulate energy production or disrupt power supplies.

The potential for such attacks underscores the need for stringent security measures in the burgeoning smart energy sector.

This threat not only poses risks to energy stability but also highlights broader implications for national security as reliance on renewable technologies increases.

CyberSecurity Advisors Network

NEWS:

16. US Soldier Intends to Admit Hacking 15 Telecom Carriers

Original Source: Dark Reading by Kristina Beek

A US soldier has signalled intentions to plead guilty to hacking into the systems of 15 telecom carriers, exposing significant vulnerabilities in telecommunications security.

This case highlights the risk of insider threats where individuals exploit their technical skills and security clearances to access sensitive information, posing serious implications for national security.

The incident has prompted authorities to reevaluate and strengthen security protocols across the telecommunications industry, emphasising the need for rigorous access controls and ongoing surveillance to prevent future breaches.

CyberSecurity Advisors Network

NEWS:

17. Qilin ransomware claims attack at Lee Enterprises, leaks stolen data

Original Source: BleepingComputer by Bill Toulas

Qilin ransomware has targeted Lee Enterprises, marking a significant breach in media cybersecurity.

The group behind the attack has not only encrypted the company's data but also begun leaking sensitive information to pressure for a ransom.

This incident highlights the increasing threat ransomware poses to the media sector, where disruptions can significantly impact operations and information integrity.

Lee Enterprises is currently assessing the damage and coordinating with cybersecurity experts to mitigate the effects, reinforce their defenses, and prevent future attacks.

CyberSecurity Advisors Network

NEWS:

18. Amnesty Finds Cellebrite's Zero-Day Used to Unlock Serbian Activist's Android Phone

Original Source: The Hacker News by Ravie Lakshmanan

Amnesty International has reported that a zero-day exploit in Cellebrite's forensic technology was used to unlawfully access the Android phone of a Serbian activist.

This breach underscores significant privacy concerns and the potential for misuse of surveillance tools.

The exploit enabled unauthorised access to sensitive personal data, exposing vulnerabilities in technologies that are commonly used by law enforcement worldwide.

This incident has intensified calls for more stringent regulations on digital surveillance tools to prevent their use in political repression or other harmful activities, advocating for an international effort to protect digital rights and ensure privacy.

CyberSecurity Advisors Network

NEWS:

19. Meta apologises over flood of gore, violence and dead bodies on Instagram

Original Source: The Guardian by Dan Milmo

Meta has issued an apology following a surge of disturbing content on Instagram, including graphic violence and images of deceased individuals.

This influx has sparked widespread criticism and raised questions about the platform's content moderation policies.

Meta has acknowledged the distress caused to users and is reviewing its algorithms and moderation practices to better detect and filter out such inappropriate content.

The company has reiterated a commitment to improving its systems to ensure that Instagram remains a safe space for its community, emphasising the importance of safeguarding user experience against harmful content.

CyberSecurity Advisors Network

NEWS:

20. Fake CAPTCHA PDFs Spread Lumma Stealer via Webflow, GoDaddy, and Other Domains

Original Source: The Hacker News by Ravie Lakshmanan

Cybersecurity researchers have identified a new threat where fake CAPTCHA PDFs are being used to distribute Lumma Stealer malware across multiple domains, including Webflow and GoDaddy.

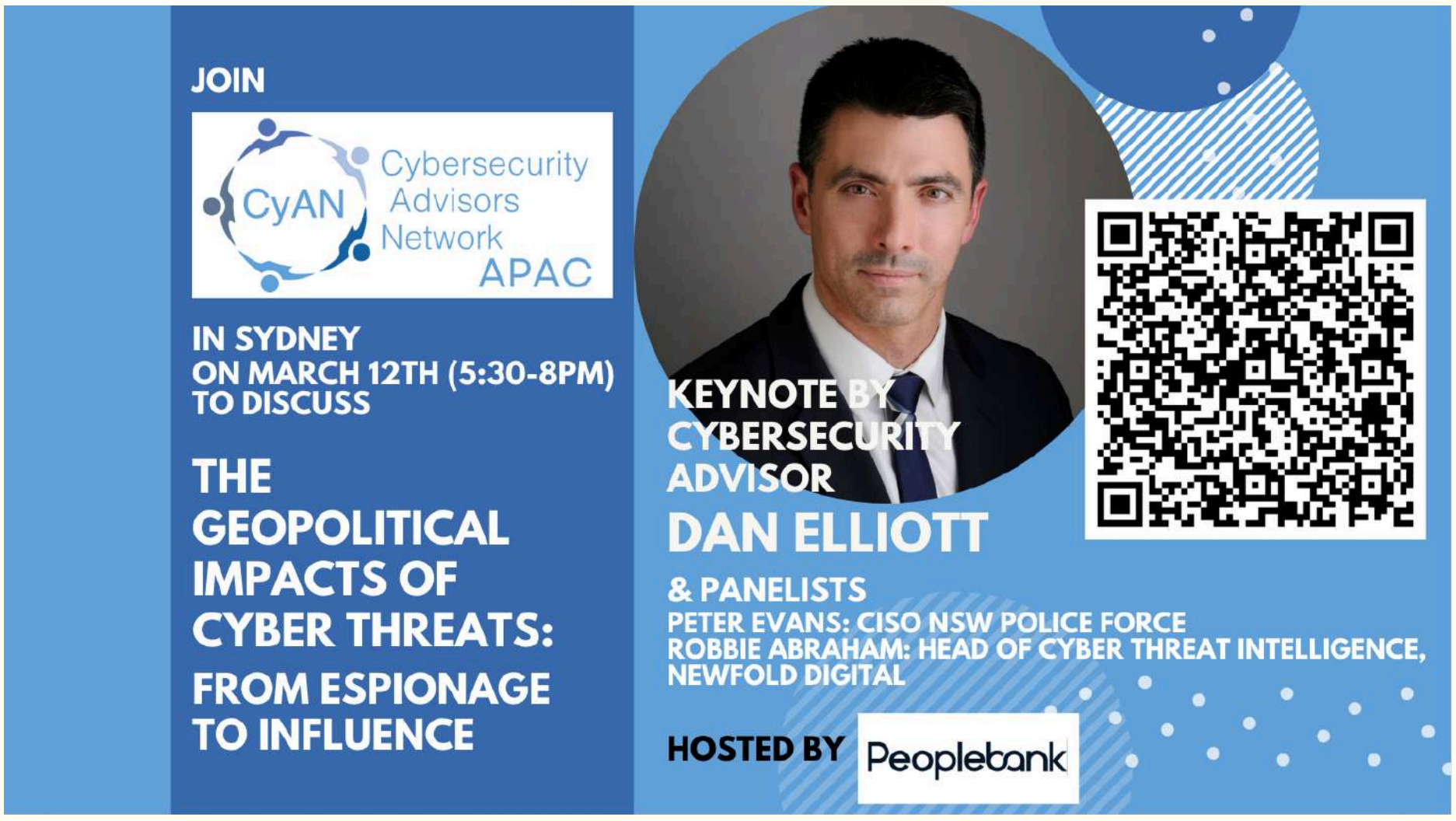
This sophisticated scheme tricks users into downloading malware under the guise of verifying identity, exploiting trusted website functionalities.

The Lumma Stealer can extract a wide range of personal information, leading to significant privacy breaches.

Experts are urging users to be cautious with downloads and to verify the authenticity of files and requests, especially when prompted by unexpected security checks.

CyberSecurity Advisors Network

SAVE THE DATE!



Mark your calendars—this is one event you won't want to miss!

In a world where cyber threats are reshaping global power dynamics, understanding their geopolitical implications has never been more critical. This event will provide unique insights into how the evolving cyber landscape impacts nations, organisations, and individuals, offering strategies to navigate these challenges with clarity and resilience.

We'll begin with a keynote from acclaimed cybersecurity advisor Dan Elliott, followed by a panel discussion moderated by Dr. Saba Bagheri, Cyber Threat Intelligence Manager at BUPA, featuring

- **Peter Evans, CISO at NSW Police Force**
- **Robbie Abraham, Head of Cyber Threat Intelligence at Newfold Digital**

NEWS:

21. Microsoft Disrupted a Global Cybercrime Ring Abusing Azure OpenAIService

Original Source: Security Affairs by Pierluigi Paganini

Microsoft has successfully disrupted a global cybercrime ring that was abusing its Azure OpenAI service.

The operation involved cybercriminals using the service for malicious activities, including phishing and spreading malware.

Microsoft's intervention highlights the ongoing battle against cyber threats exploiting cloud platforms. The company's proactive measures have prevented further misuse, demonstrating the critical need for continuous monitoring and rapid response capabilities in cloud services.

This event underscores the importance of vigilance and technological readiness in thwarting cybercriminal activities that leverage powerful cloud-based tools.

CyberSecurity Advisors Network

NEWS:

22. Farm and Food Cybersecurity Act reintroduced to protect food supply chain from cyber threats

Original Source: Industrial Cyber by Anna Ribeiro

The US Farm and Food Cybersecurity Act has been reintroduced to bolster cybersecurity across the food supply chain.

This legislative push aims to protect critical infrastructure from cyber threats that could disrupt food production and distribution.

The act calls for enhanced security protocols, collaboration between government agencies and private sectors, and increased funding for cybersecurity measures.

This initiative highlights the growing recognition of the vulnerability of the agricultural sector to cyber attacks, emphasising the importance of safeguarding this essential industry from potential disruptions.

CyberSecurity Advisors Network

NEWS:

23. Over 49,000 misconfigured building access systems exposed online

Original Source: BleepingComputer by Bill Toulas

Over 49,000 building access control systems have been found exposed online due to misconfigurations, posing a significant security risk.

These systems, which manage entry to facilities, could potentially allow unauthorised access if exploited by cybercriminals.

The exposure highlights a widespread issue in the security practices surrounding building management systems and underscores the need for stringent security audits and configurations.

Cybersecurity experts are calling for immediate action to address these vulnerabilities to prevent potential breaches that could compromise both physical and data security.

CyberSecurity Advisors Network

NEWS:

24. Hegseth orders Cyber Command to stand down on Russia planning

Original Source: The Record by Martin Matishak

In a controversial move, Hegseth has instructed Cyber Command to stand down on planning any aggressive cyber operations against Russia.

This directive aligns with a broader strategy shift but has raised concerns among cybersecurity experts about the potential consequences for global cyber defence.

Critics argue that pulling back from proactive cyber measures against a known adversary could weaken the overall security posture and embolden malicious cyber activities by state-sponsored groups.

The decision is seen as a step back in maintaining robust cyber deterrence and protecting national interests.

CyberSecurity Advisors Network

ANALYSIS:

25. Third-Party Risk Top Cybersecurity Claims

Original Source: Dark Reading by Robert Lemos

Recent findings reveal that third-party risks now lead as the primary cause of cybersecurity claims, underscoring the significant vulnerabilities associated with external collaborations.

These risks stem from inadequate security measures among vendors and partners, potentially leading to data breaches and substantial financial losses.

The rise in such claims highlights the necessity for organizations to enhance their third-party risk management protocols, ensuring rigorous security assessments and continuous monitoring of external entities.

This proactive approach is essential to safeguard sensitive data and maintain robust cybersecurity defenses in an interconnected business environment.

CyberSecurity Advisors Network

CyAN Members-Only Quiz Challenge

Are You In the #CyANQuiz?

Hey CyAN Champions,

Ready to test your cybersecurity know-how? Join our Quarterly #CyANQuiz Challenge, starting this March!

Each quiz offers a chance to **climb higher on the leaderboard**, with points accumulating throughout the year.

🔥 **Engaging Challenges:** Tackle tough cybersecurity questions and sharpen your expertise.

🏆 **Compete for Glory:** Match wits with fellow CyAN pros quarterly and vie for awesome prizes and exclusive CyAN perks!

📅 **Mark Your Calendar:** Kick off is March 31st!

Compete throughout the year with each quiz adding to your total score. **Top year-end champions win big rewards (free membership for a year anyone!)!**

Join the fun—this isn't just a quiz, it's a year-long challenge to **shine in the CyAN community**.

Are you ready? **Check your email for further details!**

ANALYSIS:

26. Top 10 Most Probable Ways a Company Can Be Hacked

Original Source: Dark Reading by Erich Kron

Cybersecurity expert Erich Kron has compiled a list of the top ten most probable ways companies can fall victim to hackers.

This list serves as a crucial guide for businesses aiming to bolster their cyber defences. The vulnerabilities range from phishing and malware to weak passwords and unsecured remote access.

Kron emphasises the importance of awareness and proactive measures, such as regular updates, training employees, and implementing strong access controls.

Highlighting these common vulnerabilities aims to empower companies to better protect themselves from increasingly sophisticated cyber threats.

CyberSecurity Advisors Network

ANALYSIS:

27. This 5-year tech industry forecast predicts some surprising winners - and losers

Original Source: ZDNet by Joe McKendrick

A recent five-year forecast for the tech industry has identified potential winners and losers, shedding light on expected shifts in market dynamics.

The report predicts that emerging technologies like artificial intelligence and blockchain will see significant growth, while traditional sectors may face challenges adapting to rapid technological changes.

Analysts stress the importance of innovation and flexibility for companies aiming to thrive in this evolving landscape.

The forecast serves as a strategic guide for stakeholders to anticipate changes and strategically position themselves for success in the competitive tech arena.

CyberSecurity Advisors Network

ANALYSIS:

28. 3 Things to Know About AI Data Poisoning

Original Source: Dark Reading by Arvind Nithrakashyap

AI data poisoning is emerging as a critical cybersecurity threat, allowing attackers to manipulate machine learning models by corrupting their training data.

This technique can degrade AI performance, introduce biases, or even cause systems to make harmful decisions.

Security experts warn that as AI becomes more integrated into critical sectors like healthcare, finance, and cybersecurity, the risk of poisoned data grows.

Organizations are urged to implement robust data validation, adversarial testing, and security protocols to safeguard AI integrity and prevent malicious exploitation of AI-driven technologies.

CyberSecurity Advisors Network

ANALYSIS:

29. Fortifying Financial Services Cybersecurity with Threat Intelligence and Cybersecurity Automation

Original Source: Financial IT by Chris Jacob

The financial sector is ramping up cybersecurity efforts by integrating threat intelligence and automation to combat increasingly sophisticated cyber threats.

Experts highlight how automation enhances threat detection and response times, reducing reliance on manual processes that leave institutions vulnerable.

By leveraging AI-driven security measures, financial firms can better predict, prevent, and mitigate cyber attacks.

As cybercriminal tactics evolve, industry leaders emphasise the necessity of real-time intelligence and automated defenses to protect sensitive financial data and maintain customer trust.

CyberSecurity Advisors Network

CyAN CyAN Members
Op Eds, Articles, etc

30. The Cost of Silence: Enhancing Cyber Safety to Address Domestic Violence's Impact on Women's Employment and Education

By CyAN Global Vice President, Kim Chandler McDonald

CyAN Global VP Kim Chandler McDonald explores how technology-facilitated abuse disrupts women's employment and education, limiting financial independence and career growth.

She highlights the role of digital safety in preventing coercive control and ensuring that survivors can access opportunities without fear of online harassment.

The article advocates for stronger policies, employer awareness, and cybersecurity solutions that protect at-risk individuals.

By addressing these challenges, Kim underscores the urgent need for systemic changes to create safer digital spaces and empower affected women.

CyberSecurity Advisors Network

CyAN CyAN Members
Op Eds, Articles, etc

31. Open Letter – Support for Responsible Cybersecurity Vulnerability Disclosure in German

By CyAN Staff

CyAN staff have issued an open letter advocating for responsible cybersecurity vulnerability disclosure in Germany, emphasising the need for clear legal protections for security researchers.

The letter highlights concerns that without proper safeguards, ethical hackers may face legal repercussions for exposing security flaws.

CyAN calls for legislation that encourages transparency, cooperation, and responsible reporting to strengthen Germany's cybersecurity posture.

The initiative aims to balance security needs with ethical considerations, ensuring researchers can contribute without fear of prosecution.

CyberSecurity Advisors Network

CyAN CyAN Members
Op Eds, Articles, etc

32. How MITRE ATT&CK Helps Us Understand and Stop Cyber Threats

By CyAN Fel Gayanilo

CyAN General Secretary Fel Gayanilo explores how the MITRE ATT&CK framework enhances cybersecurity by providing a structured way to identify, analyse, and mitigate cyber threats.

The framework helps security teams understand attacker tactics, techniques, and procedures, enabling more effective threat detection and response.

Fel highlights its role in improving incident response, refining threat intelligence, and strengthening organisational security postures.

As cyber threats evolve, he emphasises that leveraging frameworks like MITRE ATT&CK is crucial for staying ahead of adversaries and proactively defending critical systems.

CyberSecurity Advisors Network

CyAN Member's News:

We at CyAN are ALWAYS overjoyed to celebrate our members successes and their contributions to the cybersecurity community!

We're immensely proud to share that two esteemed members of the CyAN community, CyAN member Mohit Makhija and CyAN APAC Director Saba Bagheri, are finalists in the prestigious 2025 Australian Cyber Awards!

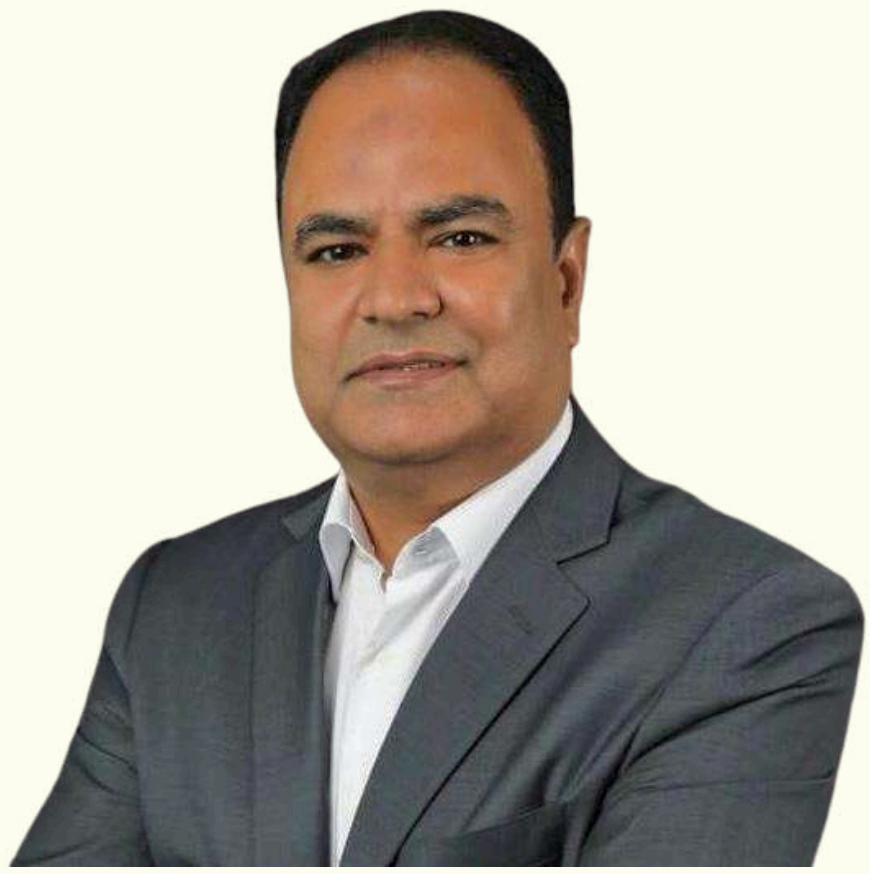
Mohit has been recognised in the Cyber Security Professional of the Year category, while Saba has earned accolades in both the Cyber Security Consultant of the Year - Enterprise and Cyber Security Professional of the Year - Government and Defence categories.

Their nominations are a testament to their outstanding contributions and dedication to the field of cybersecurity. Join us in congratulating Mohit and Saba—we are rooting for their success and celebrate their well-deserved recognition!

CyAN Member's News:

And there's more!

Please join us in celebrating our valued member Mohammed Shakil Khan who has earned his Independent Director Certification from IICA and is now a part of the Independent Director's Databank of Ministry of Corporate Affairs, Govt. of India.



Congratulations, Mohammed!

We're excited to celebrate your achievement in earning the Independent Director Certification from the Indian Institute of Corporate Affairs (IICA) and becoming part of the Independent Director's Databank under the Ministry of Corporate Affairs, Govt. of India.

This milestone reflects your dedication to corporate governance and leadership. Wishing you continued success in making an impact!

CyberSecurity Advisors Network

UPCOMING CyAN and CyAN Partner EVENTS:

- **Breaking the Cycle: Combating Online IBSA for a Safer Digital Experience webinar, March 6th (EST 6AM, CET 12PM, AEST 10PM)**
- **CyAN APAC: The Geopolitical Impacts of Cyber Threats: From Espionage to Influence keynote by Dan Elliot, March 12, Peoplebank, Sydney (save the date, more info on page 10 of this newsletter!)**
- **Trust & Safety Forum at Forum INCYBER Europe (FIC), Lille, France: April 1-2**
- **GITEX AFRICA, Marrakesh, Morocco: 14-16 April**
- **GITEX ASIA: Singapore (Marina Bay Sands) 23-25 April**
- **GISEC: Dubai Word Trade Center, Dubai, UAE: 6- 8 May**
- **The Cyber Outstanding Security Performance Awards (Cyber OSPAs), May 8, London, UK**
- **World AI Technology Expo UAE, Dubai, UAE: 14-15 May 2025 https://worldaiexpo.i**
- **MaTeCC, Rabat, Morocco: 7-9 June, 2025**

CyAN Cybersecurity Advisors Network

Catch up on Past Issues:

Missed an issue of (In)Securities? No worries! Scan the QR code to explore our archive of past editions—packed with insights, trends, and actionable tips to keep you ahead in the ever-evolving world of cybersecurity. Dive in and catch up today!

CyberSecurity Advisors Network

If you found this interesting, please like and share it with your friends and colleagues!

#ReallyInterestingCyberStuff!
#SharingIsCaring